(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10303945 A**

(43) Date of publication of application: **13 . 11 . 98**

(51) Int. Cl **H04L 12/40**
G11B 20/10
H04L 9/08
H04L 9/14
H04L 9/16
H04L 12/56

(21) Application number: **09106105**

(22) Date of filing: **23 . 04 . 97**

(71) Applicant: **SONY CORP**

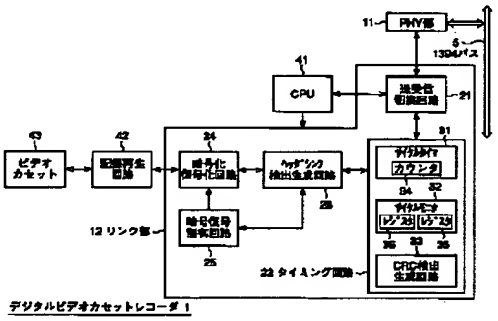
(72) Inventor: **OSAKABE YOSHIO**
SATO MAKOTO
OSAWA YOSHITOMO
ASANO TOMOYUKI
ISHIGURO RYUJI
SHIMA HISATO

(54) **DATA TRANSMITTING DEVICE AND METHOD, DATA RECEIVING DEVICE AND METHOD, DATA TRANSMITTING/RECEIVING SYSTEM AND METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent unauthorized utilization of data.

SOLUTION: The data to be transmitted with a 1394 bus 5 is ciphered by a ciphering and deciphering circuit 24 and a header is added to the data by a header sync detecting and generating circuit 23. After a CRC is added to the data by a CRC detecting and generating circuit 33, the data is packetted to an isochronous packet in an isochronous mode by a transmission/reception switching circuit 21. Among ciphering keys, a session key is transmitted by a packet in an asynchronous mode and a time variable key is transmitted by a packet in the isochronous mode.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－303945

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/40		Ｈ０４Ｌ　11/00	３２０
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
			Ｄ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｃ
9/14			６４１

審査請求　未請求　請求項の数21　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平9－106105

(22)出願日　平成９年(1997)４月23日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　刑部　義雄
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　佐藤　真
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　弁理士　稲本　義雄

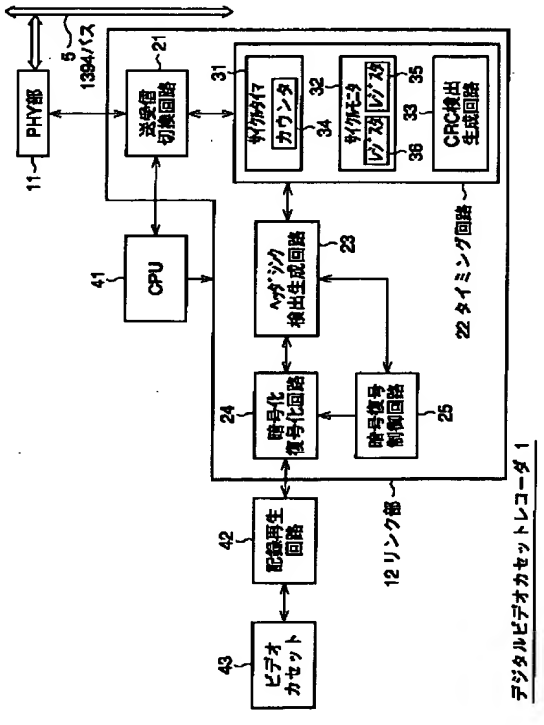
最終頁に続く

(54)【発明の名称】　データ送信装置および方法、データ受信装置および方法、並びにデータ送受信システムおよび方法

(57)【要約】

【課題】　データの不正な利用を防止する。

【解決手段】　１３９４バス５を介して伝送するデータを、暗号化復号化回路２４で暗号化し、ヘッダシンク検出生成回路２３でヘッダを付加する。CRC検出生成回路３３でCRCを付加した後、送受信切換回路２１でアイソクロナスモードのアイソクロナスパケットにパケット化する。暗号鍵のうち、セッションキーは、アシンクロナスモードのパケットで伝送し、時変キーは、アイソクロナスモードのパケットで伝送する。



1

【特許請求の範囲】

【請求項１】　アイソクロナスモードとアシンクロナスモードとを有するシリアルバスで接続された情報処理装置にデータを送信するデータ送信装置において、
送信するデータを暗号鍵を用いて暗号化する暗号化手段と、
前記暗号化手段により暗号化されたデータを、前記アイソクロナスモードのパケットにパケット化するパケット化手段と、
前記パケット化手段によりパケット化されたデータを前記シリアルバスに送信する送信手段とを備えることを特徴とするデータ送信装置。

【請求項２】　前記パケットのヘッダに、前記暗号化に関する識別コードを記録する記録手段をさらに備えることを特徴とする請求項１に記載のデータ送信装置。

【請求項３】　前記暗号鍵は、送信するデータの各セッションにおいて不変なセッションキーと、前記セッション内において更新される時変キーとからなることを特徴とする請求項１に記載のデータ送信装置。

【請求項４】　前記時変キーに関する情報を、前記アイソクロナスモードのパケットに記録する記録手段をさらに備えることを特徴とする請求項３に記載のデータ送信装置。

【請求項５】　前記記録手段は、前記時変キーに関する情報を、前記パケットのヘッダに記録することを特徴とする請求項４に記載のデータ送信装置。

【請求項６】　前記パケットに含ませるデータから所定のデータを前記時変キーとして抽出する抽出手段をさらに備えることを特徴とする請求項３に記載のデータ送信装置。

【請求項７】　前記時変キーとして抽出するデータを含ませる前記パケットは、前記シリアルバスにおいて、各アイソクロナスサイクルのスタートのタイミングを表すスタートパケットであることを特徴とする請求項６に記載のデータ送信装置。

【請求項８】　前記セッションキーに関する情報を、前記アシンクロナスモードのパケットに記録する記録手段をさらに備えることを特徴とする請求項３に記載のデータ送信装置。

【請求項９】　前記暗号鍵に関する情報を、前記シリアルバスにおいて、各アイソクロナスサイクルのスタートのタイミングを表すスタートパケットに記録する記録手段をさらに備えることを特徴とする請求項１に記載のデータ送信装置。

【請求項１０】　アイソクロナスモードとアシンクロナスモードとを有するシリアルバスで接続された情報処理装置にデータを送信するデータ送信方法において、
送信するデータを暗号鍵を用いて暗号化する暗号化ステップと、
前記暗号化ステップにより暗号化されたデータを、前記

2

アイソクロナスモードのパケットにパケット化するパケット化ステップと、
前記パケット化ステップでパケット化されたデータを前記シリアルバスに送信する送信ステップとを備えることを特徴とするデータ送信方法。

【請求項１１】　アイソクロナスモードとアシンクロナスモードとを有するシリアルバスで接続されたデータ送信装置から送信されてきたデータを受信するデータ受信装置において、
前記シリアルバスを介して送信されてきたデータを受信する受信手段と、
前記アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、
前記アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段とを備えることを特徴とするデータ受信装置。

【請求項１２】　前記パケットのヘッダから、前記暗号化に関する識別コードを抽出する抽出手段をさらに備えることを特徴とする請求項１１に記載のデータ受信装置。

【請求項１３】　前記暗号鍵は、送信するデータの各セッションにおいて不変なセッションキーと、前記セッション内において更新される時変キーとからなることを特徴とする請求項１１に記載のデータ受信装置。

【請求項１４】　前記時変キーに関する情報を、前記アイソクロナスモードのパケットから抽出する抽出手段をさらに備えることを特徴とする請求項１３に記載のデータ受信装置。

【請求項１５】　前記抽出手段は、前記時変キーに関する情報を、前記パケットのヘッダから抽出することを特徴とする請求項１４に記載のデータ受信装置。

【請求項１６】　前記抽出手段は、前記パケットのデータから所定のデータを前記時変キーとして抽出することを特徴とする請求項１４に記載のデータ受信装置。

【請求項１７】　前記抽出手段が前記時変キーを抽出する前記パケットは、前記シリアルバスにおいて、各アイソクロナスサイクルのスタートのタイミングを表すスタートパケットであることを特徴とする請求項１６に記載のデータ受信装置。

【請求項１８】　前記セッションキーに関する情報を、前記アシンクロナスモードのパケットから抽出する抽出手段をさらに備えることを特徴とする請求項１３に記載のデータ受信装置。

【請求項１９】　アイソクロナスモードとアシンクロナスモードとを有するシリアルバスで接続されたデータ送信装置から送信されてきたデータを受信するデータ受信方法において、
前記シリアルバスを介して送信されてきたデータを受信する受信ステップと、

前記アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化ステップと、

前記アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号ステップとを備えることを特徴とするデータ受信方法。

【請求項２０】　アイソクロナスモードとアシンクロナスモードとを有するシリアルバスで接続されたデータ送信装置と、前記データ送信装置が送信したデータを受信するデータ受信装置とを備えるデータ送受信システムにおいて、

前記データ送信装置は、

送信するデータを暗号鍵を用いて暗号化する暗号化手段と、

前記暗号化手段により暗号化されたデータを、前記アイソクロナスモードのパケットにパケット化するパケット化手段と、

前記パケット化手段によりパケット化されたデータを前記シリアルバスに送信する送信手段とを備え、

前記データ受信装置は、

前記シリアルバスを介して送信されてきたデータを受信する受信手段と、

前記アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、

前記アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段とを備えることを特徴とするデータ送受信システム。

【請求項２１】　アイソクロナスモードとアシンクロナスモードとを有するシリアルバスで接続されたデータ送信装置と、前記データ送信装置から送信したデータを受信するデータ受信装置とを備えるデータ送受信システムのデータ送受信方法において、

前記データ送信装置は、

送信するデータを暗号鍵を用いて暗号化する暗号化ステップと、

前記暗号化ステップにより暗号化されたデータを、前記アイソクロナスモードのパケットにパケット化するパケット化ステップと、

前記パケット化ステップによりパケット化されたデータを前記シリアルバスに送信する送信ステップとを備え、

前記データ受信装置は、

前記シリアルバスを介して送信されてきたデータを受信する受信ステップと、

前記アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化ステップと、

前記アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号ステップとを備えることを特徴とするデータ送受信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ送信装置および方法、データ受信装置および方法、並びにデータ送受信システムおよび方法に関し、特に、１３９４シリアルバスを利用してデータを送受信する場合において、データが不正に利用されるのを防止するようにした、データ送信装置および方法、データ受信装置および方法、並びにデータ送受信システムおよび方法に関する。

【０００２】

【従来の技術】最近、IEEEで規定しているIEEE１３９４ハイパフォーマンスシリアルバス（以下、単に１３９４バスと称する）が普及しつつある。この１３９４バスにおいては、そこに、いわゆるAV機器や、パーソナルコンピュータなどの電子機器を接続することにより、高速にデジタルの映像や音声信号を制御コマンドとともに、実時間で１本のケーブルで伝送することができる。

【０００３】

【発明が解決しようとする課題】１３９４バスにおいて、データを伝送するのに、アシンクロナスモード（非同期データ伝送モード）と、１３９４バスのサイクルマスタが発生する８kHz（１２５μｓ）のアイソクロナスサイクルに同期するアイソクロナスモード（同期データ伝送モード）がある。コマンドは、アシンクロナスモードで伝送されることが多いが、映像信号や音声信号は、実時間で再生する必要があるため、通常、アイソクロナスモードで伝送される。

【０００４】しかしながら、このアイソクロナスモードにおける伝送は、データの送信先を指定しない、いわゆる同報通信で行われる。このため、著作権の保護を受けるべき映像信号や音声信号が１３９４バスに伝送されてしまうと、著作権者からの許諾を得ていないユーザが、不当に映像信号や音声信号をコピーしたり、これを利用して、変更や修正を加える恐れがある。

【０００５】本発明はこのような状況に鑑みてなされたものであり、不正な利用を、より確実に防止することができるようにするものである。

【０００６】

【課題を解決するための手段】請求項１に記載のデータ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化手段と、暗号化手段により暗号化されたデータを、アイソクロナスモードのパケットにパケット化するパケット化手段と、パケット化手段によりパケット化されたデータをシリアルバスに送信する送信手段とを備えることを特徴とする。

【０００７】請求項１０に記載のデータ送信方法は、送信するデータを暗号鍵を用いて暗号化する暗号化ステップと、暗号化ステップにより暗号化されたデータを、ア

5

イソクロナスモードのパケットにパケット化するパケット化ステップと、パケット化ステップでパケット化されたデータをシリアルバスに送信する送信ステップとを備えることを特徴とする。

【０００８】請求項１１に記載のデータ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段と、アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段とを備えることを特徴とする。

【０００９】請求項１９に記載のデータ受信方法は、シリアルバスを介して送信されてきたデータを受信する受信ステップと、アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化ステップと、アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号ステップとを備えることを特徴とする。

【００１０】請求項２０に記載のデータ送受信システムは、データ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化手段と、暗号化手段により暗号化されたデータを、アイソクロナスモードのパケットにパケット化するパケット化手段と、パケット化手段によりパケット化されたデータをシリアルバスに送信する送信手段とを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段と、アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段と、アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段とを備えることを特徴とする。

【００１１】請求項２１に記載のデータ送受信方法は、データ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化ステップと、暗号化ステップにより暗号化されたデータを、アイソクロナスモードのパケットにパケット化するパケット化ステップと、パケット化ステップによりパケット化されたデータをシリアルバスに送信する送信ステップとを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信ステップと、アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化ステップと、アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号ステップとを備えることを特徴とする。

【００１２】請求項１に記載のデータ送信装置および請求項１０に記載のデータ送信方法においては、暗号化されたデータが、アイソクロナスモードのパケットにパケット化されて送信される。

6

【００１３】請求項１１に記載のデータ受信装置および請求項１９に記載のデータ受信方法においては、アイソクロナスモードのパケットでパケット化して得たデータであって、暗号化されているデータが復号される。

【００１４】請求項２０に記載のデータ送受信システムおよび請求項２１に記載のデータ送受信方法においては、データ送信装置が、暗号化したデータを、アイソクロナスモードのパケットにパケット化して、シリアルバスでデータ受信装置に送信する。データ受信装置は、アイソクロナスモードのパケットでパケット化して得たデータであって、暗号化されているデータを復号する。

【００１５】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１６】請求項１に記載のデータ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化手段（例えば、図２の暗号化復号化回路２４）と、暗号化手段により暗号化されたデータを、アイソクロナスモードのパケットにパケット化するパケット化手段（例えば、図２の送受信切換回路２１）と、パケット化手段によりパケット化されたデータをシリアルバスに送信する送信手段（例えば、図２のPHY部１１）とを備えることを特徴とする。

【００１７】請求項２に記載のデータ送信装置は、パケットのヘッダに、暗号化に関する識別コードを記録する記録手段（例えば、図２の暗号復号制御回路２５）をさらに備えることを特徴とする。

【００１８】請求項４に記載のデータ送信装置は、時変キーに関する情報を、アイソクロナスモードのパケットに記録する記録手段（例えば、図２の暗号復号制御回路２５）をさらに備えることを特徴とする。

【００１９】請求項６に記載のデータ送信装置は、パケットに含ませるデータから所定のデータを時変キーとして抽出する抽出手段（例えば、図２のタイミング回路２２）をさらに備えることを特徴とする。

【００２０】請求項８に記載のデータ送信装置は、セッションキーに関する情報を、アシンクロナスモードのパケットに記録する記録手段（例えば、図２のCPU４１）をさらに備えることを特徴とする。

【００２１】請求項９に記載のデータ送信装置は、暗号鍵に関する情報を、シリアルバスにおいて、各アイソクロナスサイクルのスタートのタイミングを表すスタートパケットに記録する記録手段（例えば、図２の暗号復号制御回路２５）をさらに備えることを特徴とする。

【００２２】請求項１１に記載のデータ受信装置は、シ

リアルバスを介して送信されてきたデータを受信する受信手段（例えば、図２のPHY部１１）と、アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段（例えば、図２の送受信切換回路２１）と、アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段（例えば、図２の暗号化復号化回路２４）とを備えることを特徴とする。

【００２３】請求項１２に記載のデータ受信装置は、パケットのヘッダから、暗号化に関する識別コードを抽出する抽出手段（例えば、図２のヘッダシンク検出生成回路２３）をさらに備えることを特徴とする。

【００２４】請求項１４に記載のデータ受信装置は、時変キーに関する情報を、アイソクロナスモードのパケットから抽出する抽出手段（例えば、図２のヘッダシンク検出生成回路２３）をさらに備えることを特徴とする。

【００２５】請求項１８に記載のデータ受信装置は、セッションキーに関する情報を、アシンクロナスモードのパケットから抽出する抽出手段（例えば、図２のCPU４１）をさらに備えることを特徴とする。

【００２６】請求項２０に記載のデータ送受信システムは、データ送信装置は、送信するデータを暗号鍵を用いて暗号化する暗号化手段（例えば、図２の暗号化復号化回路２４）と、暗号化手段により暗号化されたデータを、アイソクロナスモードのパケットにパケット化するパケット化手段（例えば、図２の送受信切換回路２１）と、パケット化手段によりパケット化されたデータをシリアルバスに送信する送信手段（例えば、図２のPHY部１１）とを備え、データ受信装置は、シリアルバスを介して送信されてきたデータを受信する受信手段（例えば、図２のPHY部１１）と、アイソクロナスモードのパケットにパケット化されているデータをデパケット化するデパケット化手段（例えば、図２の送受信切換回路２１）と、アイソクロナスモードのパケットをデパケット化して得たデータであって、暗号化されているデータを復号する復号手段（例えば、図２の暗号化復号化回路２４）とを備えることを特徴とする。

【００２７】図１は、本発明を適用した情報処理システムの構成例を表している。このシステムにおいては、デジタルビデオカセットレコーダ１、テレビジョン受像機２、パーソナルコンピュータ３、およびDVDプレーヤ４が、１３９４バス５により、相互に接続されている。

【００２８】図２は、デジタルビデオカセットレコーダ１の内部の構成例を表している。PHY部１１は、１３９４バス５から伝送されてきたデータを受信し、復調して、リンク部１２の送受信切換回路２１に出力するとともに、送受信切換回路２１から供給された送信すべきデータを変調して、１３９４バス５に出力する。

【００２９】リンク部１２の送受信切換回路２１は、PHY部１１から入力された信号をアシンクロナスモードのパケットと、アイソクロナスモードのパケットとに分離し、アシンクロナスモードのパケットをデパケット化し、CPU４１に出力するとともに、アイソクロナスモードのパケットをデパケット化し、タイミング回路２２に出力する。また、CPU４１より供給されたアシンクロナスモードの信号をパケット化するとともに、タイミング回路２２より供給されたデータをアイソクロナスモードのパケットにパケット化して、PHY部１１に出力する。

【００３０】タイミング回路２２は、サイクルタイマ３１、サイクルモニタ３２、およびCRC検出生成回路３３を内蔵している。サイクルタイマ３１は、カウンタ３４を内蔵しており、このカウンタ３４は、所定のクロックをカウントし、１２５μｓのアイソクロナスサイクルのタイミングを表すカウント値を生成する。サイクルモニタ３２は、レジスタ３５，３６を内蔵している。レジスタ３５には、１３９４バス５を介して伝送されてきたサイクルスタートパケットに記録されているデスティネーションオフセット（destination_offset）の値が保持される。また、レジスタ３６は、サイクルスタートパケットのサイクルタイムデータ（cycle_time_data）の値が保持される。

【００３１】CRC検出生成回路３３は、データを受信したとき、誤り検出訂正のためのCRCデータを検出し、これを用いて誤り検出訂正処理を行う。また、データを送信する場合においては、CRC検出生成回路３３は、CRCデータを伝送すべきデータに付加する処理を行う。

【００３２】ヘッダシンク検出生成回路２３は、データ受信時、タイミング回路２２より供給されたデータからヘッダとシンクを検出し、これを分離して、実データ部分を暗号化復号化回路２４に出力する。また、データを伝送する場合には、暗号化復号化回路２４に供給された送信すべきデータに、ヘッダとシンクを付加して、タイミング回路２２に出力する。

【００３３】暗号化復号化回路２４は、データ受信時、ヘッダシンク検出生成回路２３より供給されたデータを、暗号復号制御回路２５からの制御に対応して復号し、復号結果を記録再生回路４２に出力する。また、データ送信時においては、記録再生回路４２より入力されたデータを、暗号復号制御回路２５からの制御に対応して暗号化し、ヘッダシンク検出生成回路２３に出力する。暗号復号制御回路２５は、ヘッダシンク検出生成回路２３を制御し、ヘッダやデータに所定の識別データを付加させたり、抽出したりする。また暗号復号制御回路２５は、暗号化復号化回路２４の暗号化または復号化の動作を制御する。

【００３４】記録再生回路４２は、データ受信時、暗号化復号化回路２４より入力されたデータを変調し、ビデオカセット４３に記録する。また、再生時、ビデオカセット４３に記録されているデータを再生し、復調して、暗号化復号化回路２４に出力する。

【００３５】図３は、１３９４バス５に伝送されるデータのタイミングを表している。いま、例えば、デジタルビデオカセットレコーダ１が、ビデオカセット４３を再生し、その再生データをテレビジョン受像機２に伝送しているものとする。また、DVDプレーヤ４が、内蔵するDVD（ディスク）から再生したデータを１３９４バス５を介してパーソナルコンピュータ３に伝送しているものとする。デジタルビデオカセットレコーダ１が、ビデオカセット４３を再生して出力するストリームを信号ストリームＡとし、DVDプレーヤ４が、DVDを再生して出力するストリームを信号ストリームＢとする。

【００３６】いま、例えば、１３９４バス５のサイクルマスタが、デジタルビデオカセットレコーダ１であるとすると、CPU４１は、送受信切換回路２１を制御し、１３９４バス５の１２５μｓのアイソクロナスサイクルを規定するために、サイクルスタートパケットを発生させる。このサイクルスタートパケットは、図３に示すように、アイソクロナスサイクルの先頭に、S_1，S_2，・・・のように配置される。

【００３７】図６を参照して後述するように、このサイクルスタートパケットには、サイクルタイムデータ（cycle_time_data）が配置されている。このサイクルタイムデータには、サイクルタイマ３１のカウンタ３４がカウントしているカウント値が記録される。１３９４バス５に接続されているサイクルマスタ以外の電子機器は、このサイクルタイムデータを読み取り、それを内蔵するサイクルモニタのレジスタに保持させる。

【００３８】例えば、サイクルマスタが、デジタルビデオカセットレコーダ１ではなく、パーソナルコンピュータ３である場合、パーソナルコンピュータ３がサイクルスタートパケットを送信することになる。この場合、デジタルビデオカセットレコーダ１は、１３９４バス５を介して伝送されてくるサイクルスタートパケットをPHY部１１で受信し、送受信切換回路２１で、これをデパケット化する。デパケット化されたデータは、タイミング回路２２に入力される。タイミング回路２２においては、サイクルモニタ３２で、このサイクルスタートパケットに含まれるサイクルタイムデータを読み取り、その読み取った値をレジスタ３６に保持する。そして、以後、このレジスタ３６に保持した値を基準にして、１３９４バス５上のアイソクロナスサイクルの時間管理を行う。

【００３９】このようにして、１３９４バス５に接続されている各電子機器のアイソクロナスサイクルの時間軸が共通のものとされる。

【００４０】いま、デジタルビデオカセットレコーダ１とDVDプレーヤ４が、１３９４バス５を介してデータを伝送しているので、それぞれは、アイソクロナスサイクルの所定のタイミングにおいて、アイソクロナスパケットを伝送できるようにタイムスロットの割当を受けている。デジタルビデオカセットレコーダ１と、DVDプレーヤ４は、信号ストリームＡまたは信号ストリームＢを、それぞれ圧縮してパケット化し、パケット化したデータを、それぞれ割当を受けているタイムスロットのタイミングにおいて伝送する。

【００４１】例えば、デジタルビデオカセットレコーダ１は、記録再生回路４２で、ビデオカセット４３を再生し、その再生データを暗号化復号化回路２４に供給し、セッションキーＳと時変キーｉよりなる暗号鍵を用いて暗号化させる。暗号化されたデータは、ヘッダシンク検出生成回路２３に供給され、圧縮され、ヘッダが付加される。ヘッダが付加されたデータは、さらにタイミング回路２２に入力され、CRCが付加される。このCRCは、ヘッダとデータ部、それぞれに付加される。

【００４２】タイミング回路２２より出力されたデータは、送受信切換回路２１に供給され、アイソクロナスモードのパケットにパケット化される。そして、このパケットは、上述したように、割当を受けたタイムスロットのタイミングにおいて、PHY部１１から１３９４バス５に伝送される。

【００４３】このような処理が、図３に示すように、各アイソクロナスサイクル毎に行われ、信号ストリームＡの信号A_1，A_2，A_3，・・・は、各アイソクロナスサイクルの所定のタイムスロットのタイミングで、同一の符号で示すパケットとして送信される。なお、伝送するデータが存在しないアイソクロナスサイクルにおいては、空パケットa_1，a_2が伝送される。この空パケットには、実データ部が存在せず、ヘッダ部だけが存在する。

【００４４】同様のことが、DVDプレーヤ４においても行われ、信号ストリームＢの信号B_1，B_2，・・・が、異なるタイミングで、同一の符号で示すパケットとして伝送される。

【００４５】例えば、CPU４１がコマンドを送信する場合、そのコマンドが、送受信切換回路２１に入力される。送受信切換回路２１は、このコマンドをアシンクロナスモードのパケットにパケット化し、例えば、図３においてC_1，C_2のように伝送する。

【００４６】このアシンクロナスパケットは、必要に応じて伝送されるものであるので、各アイソクロナスサイクルにおいて、常に発生するものではない。

【００４７】同様に、CPU４１は、後述するように、暗号鍵のうち、セッションキーＳを、アシンクロナスパケットで伝送する。

【００４８】このように、１３９４バス５を介して伝送された信号ストリームＡは、テレビジョン受像機２で受信され、信号ストリームＢは、パーソナルコンピュータ３で受信されるのであるが、説明の便宜上、いま信号ストリームＡが、図２に示すデジタルビデオカセットレコーダ１で受信されるものとすると、そのときの動作は次

のようになる。

【００４９】すなわち、PHY部１１は、１３９４バス５を介して伝送されてきたパケットを受信し、送受信切換回路２１に供給する。送受信切換回路２１は、入力されたパケットをアイソクロナスパケットとアシンクロナスパケットに分離し、アイソクロナスパケットをデパケット化して、タイミング回路２２に出力し、アシンクロナスパケットをデパケット化し、そのデータをCPU４１に出力する。その結果、例えば、タイミング回路２２に信号ストリームＡが供給され、CPU４１にコマンドやセッションキーＳが供給される。

【００５０】タイミング回路２２のCRC検出生成回路３３は、入力されたデータをヘッダシンク検出生成回路２３に供給する。そして、CRC検出生成回路３３は、ヘッダシンク検出生成回路２３に供給されたデータからCRCを検出し、これを用いて、誤り検出訂正処理を実行する。そして、誤りが訂正されたデータをヘッダシンク検出生成回路２３に戻す。

【００５１】ヘッダシンク検出生成回路２３は、入力されたデータからヘッダを分離し、ヘッダ情報を暗号復号制御回路２５に供給し、実データ部を暗号化復号化回路２４に供給する。暗号復号制御回路２５は、ヘッダシンク検出生成回路２３が検出したヘッダに含まれる暗号化の識別データを検出し、この検出結果に対して、暗号化復号化回路２４を制御する。すなわち、この識別データが、データが暗号化されていることを示している場合には、暗号化復号化回路２４を制御し、暗号鍵を用いて復号処理を実行させる。識別データが、データが暗号化されていないことを示している場合には、暗号化処理を省略させる。

【００５２】暗号化復号化回路２４より出力されたデータは、記録再生回路４２により、所定の方式で変調され、ビデオカセット４３に供給され、記録される。

【００５３】なお、この発明の実施の形態においては、暗号化復号化回路２４における、暗号化と復号化に用いられる暗号鍵が、セッションキーＳと、時変キーｉにより構成されている。セッションキーＳは、セッション毎に（例えば、１つの映画情報毎に、あるいは、１回の再生毎に）、適宜更新される。換言すれば、同一のセッション内においては、不変の値とされる。これに対して、時変キーｉは、１つのセッション内において、頻繁に更新される。このように、セッションキーＳと時変キーｉを暗号鍵とすることで、より安全性を高めることができる。

【００５４】すなわち、例えば、セッションキーＳが盗まれたとしても、時変キーｉが不明であれば、結局暗号化されているデータを復号することができない。さらに、時変キーｉも盗まれたとしても、時変キーｉは、時々刻々と更新されるので、極めて短い時間の間だけデータを復号することができるが、それ以降は、データを復号することができなくなる。

【００５５】セッションキーＳは、図３にK_1, K_2として示すように、所定のタイミングで、アシンクロナスパケットとして伝送される。勿論、後述するように、時変キーｉと同様に、アイソクロナスパケットとして伝送することも可能である。

【００５６】図４は、アイソクロナスパケットのフォーマットを表している。同図に示すように、その先頭の２クワドレットは、アイソクロナスヘッダとされる。このヘッダの先頭には、データ長（data_length）が記録され、その次には、データフィールド（data field）中にCIPヘッダが付加されているか否かを表すtagが記録されている。tagの次には、channelが配置される。このchannelは、例えば、図３におけるストリームＡやストリームＢの識別を行うものである。

【００５７】tcodeは、パケットフォーマットを規定するものであり、アイソクロナススタートパケットの場合、１０１０（＝Ａ）とされる。次のsyは、シンクロナイジェーションコードとされ、アプリケーション毎に規定される。本発明の実施の形態においては、このsyの下位２ビットに、３２ビット乃至４０ビットで構成される時変キーｉの２ビット分が配置される。例えば、時変キーｉが３２ビットにより構成される場合、１６パケットを集めて時変キーｉが完成することになる。syの下から３ビット目には、このパケットが時変キーｉの先頭のパケットであるか否かを示すフラグを付加することができる。例えば、時変キーｉの先頭である場合、この３番目のビットが１とされ、先頭でない場合、０とされる。

【００５８】さらに、このようにsyに時変キーｉを記録する場合、tcodeに、値１１００（＝Ｃ）を設定し、時変キーｉの識別コードとすることができる。

【００５９】暗号復号制御回路２５は、ヘッダシンク検出生成回路２３の出力するヘッダ情報から、この時変キーｉを２ビットずつ集め、１６パケット分集めたとき、完成した時変キーｉを暗号化復号化回路２４に転送することになる。

【００６０】図４に示すように、アイソクロナスヘッダの２番目のクワドレットは、ヘッダCRCとされている。そして、アイソクロナスヘッダの次のデータフィールドには、２クワドレット分のCIPヘッダが配置され、その次に、コンテンツが配置される。このコンテンツが、上述したように、暗号化されたデータとなる。

【００６１】なお、MPEGの場合、このコンテンツの領域に、ソースヘッダが配置されるが、このタイムスタンプなどが記録されているソースヘッダは、暗号化しないようにする。

【００６２】データフィールドの次には、データCRCが配置されている。

【００６３】図５は、CIPヘッダの詳細な構成を表している。同図に示すように、２クワドレットのCIPヘッダ

のうち、最初のCIPヘッダ１においては、その先頭に、ヘッダの先頭であることを表すビット（＝０）が配置され、CIPヘッダ２においては、ここにビット１が配置される。すなわち、最初のビットは、EOH_n(End of CIP header)とされ、これは、CIPヘッダの最後のクワドレットであるか否かを表している。この値は、他のクワドレットが続く場合、０とされ、CIPヘッダの最後のクワドレットである場合、１とされる。

【００６４】第２番目のビットは、Form_nとされ、これは、EOHと組み合わせることで、CIPヘッダフィールドのクワドレットを表すようになされているが、この発明の実施の形態においては、データが暗号化されている場合、ここに１が設定され、暗号化されていない場合、０が記録される。

【００６５】CIPヘッダ１の第３番目乃至第８番目のビットは、SID(Source node ID)とされる。SIDの次には、DBS(Data block size in quadlets)が配置される。このDBSは、データのブロックサイズを表している。その次には、FN(Fraction number)が配置されている。これは、１つのソースパケットが分割されているブロックの数を表している。次の、QPC(Quadlet padding count)は、付加されたダミークワドレットの数を表している。次のSPH(Source packet header)は、ソースパケットがソースパケットヘッダを有しているか否かを表している。

【００６６】Rsvは、将来のために保留されている。DBCは、データブロックの損失を検知するための連続するデータブロックのカウンタの値を表している。

【００６７】FMTは、Format IDを表している。FDFは、Format dependent fieldを表している。

【００６８】図６は、サイクルスタートパケットのフォーマットを表している。その先頭には、destination_IDが配置され、これは、データ転送先のIDを表している。次のtl（transaction label）は、通常すべて０とされる。そこで、例えば、ここに時変キーｉの値を記録するようにすることができる。

【００６９】rt（retry code）は、通常０とされる。次の、tcode（transactin code）には、パケットタイプのtransaction codeが配置される。

【００７０】priは、priorityであり、１３９４バス５で接続される機器間で使用されるとき、すべて１とされる。このpriにも、時変キーｉを割り当てることが可能である。

【００７１】source_IDには、データの伝送元のIDが記録される。destination_offsetには、サイクルスタートパケットからのタイミングのずれに対応するクロックの値がセットされる。cycle_time_dataには、上述したように、サイクルマスタの基準となるレジスタの値が設定される。この値を基準として、１３９４バス５に接続されている各電子機器のアイソクロナスサイクルの時間軸

の基準が設定される。一番最後には、ヘッダのCRCが配置されている。

【００７２】以上の実施の形態においては、時変キーｉを、パケットのデータ部またはヘッダ部に書き込んで伝送するようにしたが、例えば、サイクルスタートパケットのdestination_offset，cycle_time_dataまたはheader_CRCのいずれかの値を、そのまま時変キーｉとして用いるようにすることもできる。

【００７３】また、各電子機器は、これらの値を読み取って、そのサイクルモニタ３２のレジスタ３５，３６に、これらの値を保持しているので、これらの値から時変キーｉを抽出するようにすることも可能である。

【００７４】さらにまた、図５に示したCIPヘッダのDBC、図４に示したdata_CRCの値を、そのまま時変キーｉとして用いるようにすることもできる。

【００７５】

【発明の効果】以上の如く、請求項１に記載のデータ送信装置および請求項１０に記載のデータ送信方法によれば、暗号化されたデータを、アイソクロナスモードのパケットにパケット化して、シリアルバスに送信するようにしたので、より安全にデータを送信することが可能となる。

【００７６】請求項１１に記載のデータ受信装置および請求項１９に記載のデータ受信方法によれば、アイソクロナスモードのパケットでパケット化して得たデータであって、暗号化されているデータを復号するようにしたので、安全に伝送されてきたデータを、確実に復号することが可能となる。

【００７７】請求項２０に記載のデータ送受信システムおよび請求項２１に記載のデータ送受信方法によれば、データ送信装置で暗号化されたデータを、アイソクロナスモードのパケットにパケット化して送信し、データ受信装置において、これを受信するようにしたので、安全なデータ送受信システムを実現することができる。

【図面の簡単な説明】

【図１】本発明を適用したデータ送受信システムの構成例を示すブロック図である。

【図２】図１のデジタルビデオカセットレコーダ１の内部の構成例を示すブロック図である。

【図３】１３９４バスの伝送のタイミングを説明する図である。

【図４】アイソクロナスパケットのフォーマットを示す図である。

【図５】CIPヘッダのフォーマットを示す図である。

【図６】サイクルスタートパケットのフォーマットを示す図である。

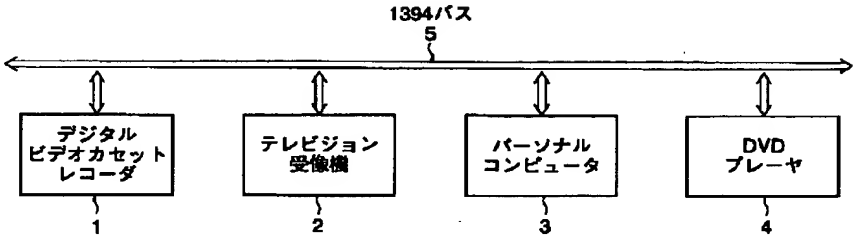
【符号の説明】

１　デジタルビデオカセットレコーダ，　２　テレビジョン受像機，　３　パーソナルコンピュータ，　４　DVDプレーヤ，　５　１３９４バス，　１１　PHY部，　１

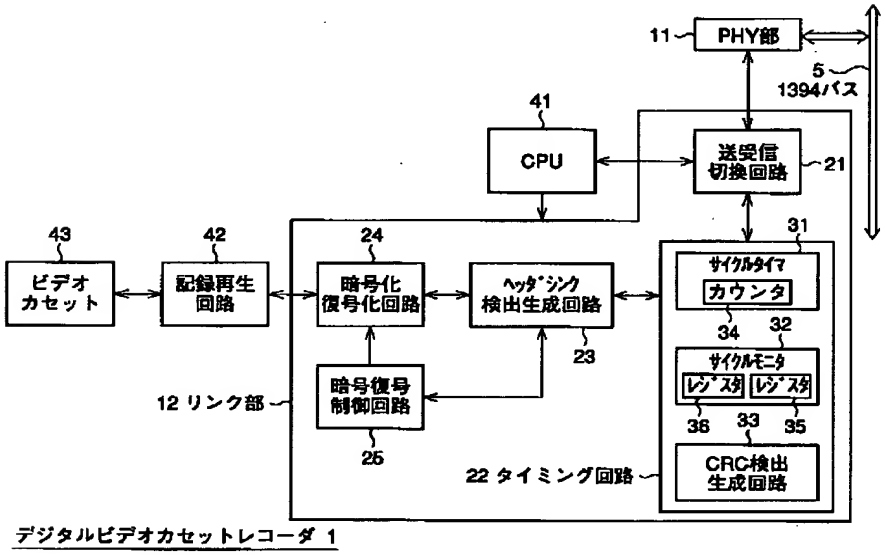
15 16

２　リンク部，　２１　送受信切換回路，　２２　タイ　　＊１　サイクルタイマ，　３２　サイクルモニタ，　３３　ミング回路，２３　ヘッダシンク検出生成回路，　２４　　CRC検出生成回路，　３４　カウンタ，　３５，３６　暗号化復号化回路，　２５　暗号復号制御回路，　３＊　　レジスタ，　４１　ＣＰＵ

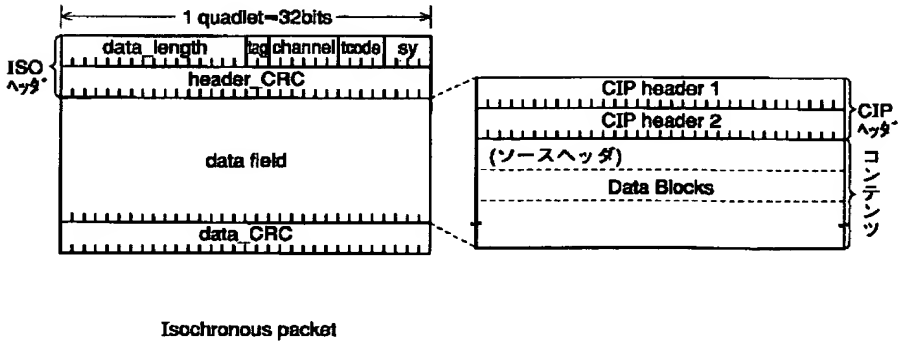
【図１】



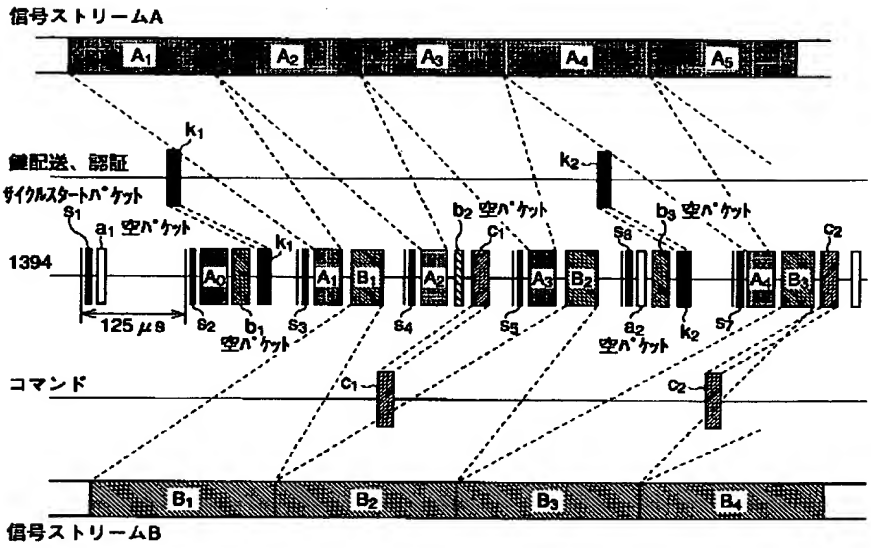
【図２】



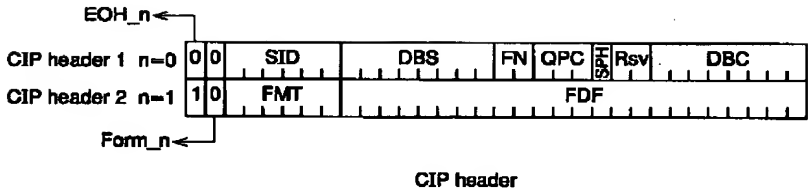
【図４】



【図３】

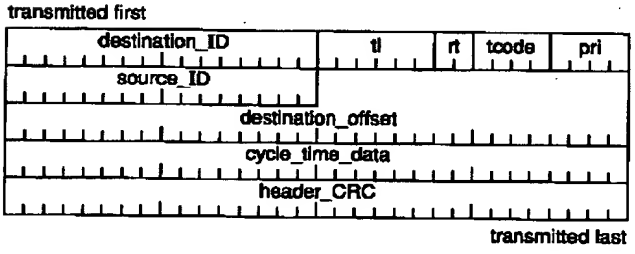


【図５】



CIP header

【図６】



Cycle start primary packet format

フロントページの続き

(51) Int. Cl. ⁶		識別記号	F I		
Ｈ０４Ｌ	9/16		Ｈ０４Ｌ	9/00	６４３
	12/56			11/20	１０２Ｆ

(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　嶋　久登
アメリカ合衆国　カリフォルニア州　サラトガ　パセオ・フローレス12610